SECURE COMPUTER COMMUNICATION

The present invention relates to a method for secure communication between computer user domains, particularly to the application of domain separators to ensure secure communication across networks.

Computing systems often comprise user domains (whether a computer or a network of computers) of different security classification on connecting networks. There is then a need to protect data communicated between user domains of the same classification from unauthorised access, whether unauthorised persons in user domains of lower classification or potential unauthorised persons in the connecting network.

Previously, user domains with different security levels have been placed on different connecting networks to prevent data packets being mis-routed to a user domain of lower security classification. However, this is disadvantageous as it does not allow bandwidth to be shared between the different security levels.

Encrypting data prior to sending it on an unsecured medium allows bandwidth to be shared. A cryptograph is used to protect the data from potential unauthorised persons in the connecting network as well as to separate user domains of different classifications from each other. While attempts to encrypt data to improve security have had some commercial success, the cryptographic devices required for high security systems are costly and difficult to produce. This is due to the need for high security system cryptographs to meet stringent requirements for reliability of implementation. These requirements are extremely difficult to satisfy in devices as complex as cryptographs, particularly with respect to cryptographic key management functions. Less robust cryptographs, while good enough for most applications, are not acceptable for use in high security systems.

There is therefore a need for an improved method of communication between user domains that provides a high degree of security in data transfers.

Accordingly, the present invention provides a method of improving the security of computer communications over a connecting network comprising the

steps carried out before a data packet enters the connecting network from a user domain, of (a) tagging the data packet with a security level marking and (b) appending the tagged data packet with a string formed from a check-sum made over the data packet and security level marking tag, to form a datagram. The string may comprise a check-sum or part of a check-sum. While not all the bits of a check-sum are required, enough bits must be used to ensure that the probability of failure due to accidental packet corruption is less than a desired threshold.

Preferably, as the datagram attempts to enter a second user domain, the method comprises the further steps of: (c) verifying the string in the received datagram matches a string calculated over the received data packet and security level marking tag and (d) verifying the received security level marking tag matches the security level of the second user domain.

Advantageously, the datagram is encrypted before entry into the connecting network. This further secures the data from unauthorised access.

Optionally, datagrams from more than one user domain are encrypted by the same cryptograph. This reduces the number of cryptographs required.

Advantageously, the string made over the data packet and security level marking tag is a one-way hash function and preferably the one-way hash function is SHA-1.

Preferably, the method further comprises the step of recording any mismatch between the string in the received datagram and a string calculated over the received data packet and security level marking tag, and any mismatch between the received security level marking tag and the security level of the second user domain. Such a security event register provides a log of data packet mis-routing or corruption.

In a further embodiment, the present invention provides a domain separator for improving the security of computer communications over a connecting network arranged to carry out the method as described above.

Optionally, the user domain security level is set by a physical switch on the domain separator. Access to the physical switch can then be restricted by physical security controls.

The invention will now be described by way of example only and with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of one embodiment of the prior art;

Figure 2 is a schematic view of an alternative prior art system;

Figure 3 is a diagrammatic illustration of an embodiment of the invention;

Figure 4 is a schematic view of another embodiment of the invention; and

Figure 5 is a schematic view of a further embodiment of the invention.

In Figure 1, user domains A_1 and A_2 with security classification level 1 (SCL1) are on a connecting network N_1 and user domains B_1 and B_2 with security classification level 2 (SCL2) are on a different connecting network N_2. SCL1 data packets can be communicated between A_1 and A_2, without the possibility of mis-routing to B_1 or B_2. Similarly, SCL2 data packets can be communicated between B_1 and B_2 without the possibility of mis-routing to A_1 or A_2. Therefore, the data is protected from unauthorised persons in user domains viewing material at a classification level higher than that to which the person is cleared. This system relies on the managers of networks N_1 and N_2 having authorisation to view SCL1 and SCL2 data packets respectively. Persons within the dashed lines 2a must be authorised to see at least SCL1 and persons within dashed lines 2b must be authorised to see at least SCL2. A system having different security levels separated onto different networks is disadvantageous as bandwidth cannot then be shared between the security levels.

Figure 2 illustrates a system architecture according to the prior art, involving the use of encryption, which circumvents the problem of bandwidth sharing. User domains A_3, A_4, B_3 and B_4 are all connected to one connecting network N_3. Plain text data within the dotted lines 6a, 6b, 6c and 6d is encrypted on leaving each user domain via cryptographs 4. For certain high

security systems the cryptographs 4 must meet high reliability requirements for security certification. Unauthorised persons in the connecting network N_3 are unable to read the encrypted data. User domains with security classification lower than that of the sender are unable to access the data as they do not hold the correct cryptographic key. As network N_3 is shared between the different classifications, the use of bandwidth is more efficient. However, this system relies on costly cryptographic devices certified for use in high security systems.

The present invention allows network bandwidth to be shared between data packets of different classifications while keeping user domains of higher security classification separate from those of lower classification. The mis-routing of data packets to user domains of lower security classification is prevented as is the delivery of corrupted data packets. In the embodiment of the present invention shown in Figure 3, a domain separator 8 encapsulates data packets from user domains A_5, A_6, B_5, B_6 with a security tag, giving an indication of the security classification of the data packet. The security tag is based on a physical switch (not shown) setting within the domain separator 8. There is no effective way for someone in a user domain to attack the domain separator without having physical access to it. In particular, the security tag is based on a physical switch setting in the domain separator which can be secured.

A check-sum is then made over the data packet and security tag for transport across a connecting network N_4. A string comprising the hash, or part of the hash, is appended to the tagged data packet. A hash may comprise of, for example, 160 bits. While not all the bits are required, enough bits must be used to ensure that the probability of failure due to accidental packet corruption is less than a desired threshold. The datagram, comprising the data packet with the security tag and the string then enters the connecting network N_4.

The check-sum algorithm is a one-way hash function, a mathematical function which operates on an arbitrary-length pre-image message and converts it into a fixed-length binary sequence, known as the hash. The one-way aspect (known as pre-image resistance) means that it is computationally infeasible to reverse the process, that is, to find a string that hashes to a given value. With a

good hash function it is computationally infeasible to find two strings which produce the same hash (known as second pre-image resistance). Small changes in an input string produce large changes in the hash. A domain separator with such a one-way hash function protects the data from unauthorised persons in the connecting network, provided the check-sum algorithm is not known to the unauthorised persons, and from accidental transport from one user domain to another of lower classification.

The preferred one-way hash function is SHA-1 (as described in the National Institute of Standards and Technology's Federal Information Processing Standards Publication 180-1) but alternatives may be used. Alternatively, a check-sum that is not a one-way hash function may be used in a domain separator that protects the data from accidental transport from one user domain to another of lower classification.

On arrival of the datagram at a destination user domain, the domain separator 8 for the destination domain removes the string from the datagram and compares it to a newly computed string of the remainder of the datagram. If the string comprises part of a hash, the same specific part of the newly computed hash is compared to the part of the hash appended to the tagged data packet. The security tag of the datagram is compared to the security setting of the destination domain separator 8. If both the security tag and the string are correct, the original data packet is delivered.

A domain separator protects the integrity of the data it encapsulates, rather than the confidentiality. It also protects the integrity of the security tag which records the protective marking of the material.

If a data packet is mis-routed in the connecting network and is delivered in error to a user domain with the wrong security level, the domain separator 8 at the destination will discard the packet if the security tag of the data packet does not match the switch setting at the destination.

Similarly, if a data packet is corrupted in transit (including corruption of the security tag) then the string in the data packet will not match the string calculated at the destination and the packet will be dropped.

A security event register (not shown) logs security events such as the discard of data packets by a domain separator.

The connecting network N_4 can be physically secured, for example riveted in conduits on a ship or in a building, to prevent access to the multi-level plain text connecting network.

Persons within the dashed lines 10a, 10b, 10c and 10d in Figure 3 must be cleared to the security classification level of the user domains A_5, A_6, B_5 and B_6, respectively. Managers of the connecting network N_4 must be cleared to the highest security classification level in the system.

If the connecting network managers are trusted, the domain separator algorithm for calculating the check-sum algorithm may be publicly known. However, if the connecting network managers can be trusted to see the data sent from one user domain to another but cannot be trusted not to corrupt the data packet (for example, changing the data packet security tag to redirect the data packet to the wrong domain), the check-sum algorithm should not be publicly known. Alternatively, encryption can be used to protect the data from unauthorised persons in the connecting network, as shown in Figures 4 and 5. The use of encryption not only prevents connecting network managers corrupting data packets but also prevents the managers from viewing the data. If the data is encrypted the check-sum algorithm can be published.

The datagram, comprising the data packet with the security tag and the hash, is encrypted on leaving the domain separator 8 before entry into the connecting network (N_5 in Figure 4, N_6 in Figure 5). The cryptographs 12 can be assigned to each user domain (A_7, A_8, B_7, B_8 in Figure 4) or to groups of user domains as illustrated in Figure 5, with one cryptograph 12 assigned to A_9 and B_9 and a second cryptograph 12 assigned to A_{10} and B_{10}. While each of the domain separators and cryptographs are referred to by the numerals 8 and 12 respectively in the figures, it is to be understood that the invention is not limited to the use of one type of domain separator or cryptograph in each embodiment.

On arrival of the encrypted datagram at a destination user domain, the datagram is decrypted and the domain separator 8 for the destination domain

verifies the check-sum and security level marking tag as described above before either allowing the data packet to enter the user domain or discarding the data packet.

Persons within dashed lines 14a, 14b, 14c, 14d, 18a, 18b, 18c and 18d must be cleared to the security classification level of user domains A_7, A_8, B_7, B_8, A_9, A_{10}, B_9 and B_{10}, respectively.

The domain separator, at the exit point of each user domain, provides a means of preventing data packets from being mis-routed to user domains of lower security classification. It is easier to produce a domain separator certified for use in high security systems than it is to produce a cryptograph certified for use in high security systems because the domain separator performs a simpler function and has no key management function. The cryptographs 12 used in conjunction with domain separators 8 are used to protect the data from unauthorised persons in the connecting network. Data packets outside dotted lines 16a, 16b, 16c, 16d, 20a and 20b are protected from unauthorised persons in the connecting network N_5 or N_6. As the cryptographs 12 in the present invention are not used for preventing the incorrect delivery of data packets, they need not meet requirements for reliability of implementation as stringent as those needed by cryptographs 4 in prior art systems where the cryptographs 4 are also used to prevent the mis-routing of data packets.